UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
08/949,525	10/14/1997	MICHAEL J. WIENER	ENT970827-1	8206

7590 01/25/2002

CHRISTOPHER J RECKAMP
Vedder Price Kaufman & Kammholz
222 North LaSalle Street
Suite 2600
Chicago, IL 60601

EXAMINER	
MEISLAHN, DOUGLAS J	
ART UNIT	PAPER NUMBER
2132	30

DATE MAILED: 01/25/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 08/949,525	Applicant(s) WIENER ET AL.	
	Examiner Douglas J. Meislahn	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 January 2002* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 11 January 2002 that amended claims 5, 19, and 25 and added claims 27-29.

Response to Arguments

2. Applicant's arguments filed 11 January 2002 have been fully considered but they are not persuasive. Applicant opines that "by a multi-client manager" distinguishes the claims from the cited art. The real issue that applicant is attempting to address is whether the claims preclude the selectable data from being provided to a key-pair recipient. Nowhere do the claims bar this. Limitations that applicant wants ascribed to the multi-client manager must be in the claims.

3. Furthermore, even if applicant is correct that the claims preclude a user from selecting data, the references cover selection by a key-issuing entity. That is, they do not stipulate the entity that chooses the expiration data. The references instruct "you" to select key lifetimes to balance cost and efficiency against security. If read by a system administrator that provides key pairs, "you" would be the multi-client manager, while, if read by a user, "you" would be a user who would then want to determine the expiry data of keys obtained from a key generator.

4. Applicant's amendments have done little to alter the claims; adding "selectable" to "predetermined percentage" would seem to create a contradiction – how could something be selectable yet predetermined? The examiner reads this as the entity doing the predetermination had several options and chose one. The examiner feels that

this is covered by predetermination in general. Thus, that particular amendment has not altered the scope of the claim.

5. With regard to the new claims, a percentage of a lifetime is necessarily a period of time and, as a result of the predetermination, selectable. Thus, the claims have already been met.

6. With respect to claim 3, Lewis teaches a system that can send out replacement keys. As such, the system can choose not to send out replacement keys, thereby denying updating a digital signature key pair on a per client basis.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-4, 6, 8-18, 20-24, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis (5761306) in view of Ellison (Generalized Certificates).

Lewis shows a public key replacement system. Figure 2 shows that both private and public keys are updated. Lewis' system causes a key switch. Lewis does not say that there are certificates with expiry data that is user selectable. Ellison talks throughout his disclosure about certificates, which are used to authenticate public keys. Certification authorities issue these certificates. On page five, Ellison says that he believes that there is a problem with CRLs. He believes, as he says in the paragraph

bridging pages five and six, certificates should each include a validity field. He goes on to say that "[i]t is up to you to decide how long you're willing to have an invalid certificate out in the world – and to define the validity period accordingly. This is a matter of normal risk management." An example of decisions made based on risk management is demonstrated by buyers of RSA's keys; users can get a short-lived key pair for free but have to pay for longer lasting keys. An e-mail message that begins on page seven and ends on page 9 of Ellison's article outlines the benefits of eliminating CRLs. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to give users the ability to define the validity period for certificates, as taught by Ellison, in the public key update system of Lewis.

Lewis anticipates additional material in claim 9. Claim 2 is shown by Ellison. Claim 3 is met by Lewis in lines 64-65 of column 7. Claim 6 is inherent to Ellison in that an interface to select validity periods is required.

9. Claims 5, 19, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis and Ellison as applied to claims 1, 14, and 21 above, and further in view of applicant's admitted prior art.

Lewis and Ellison teach the selection of key validity periods on a per client basis. They do not specify a time frame in which a client can request key updates. In lines 14 through 19 of page 2, applicant discusses a conventional public key system in which keys have a fixed default period that is " . . . generally a fixed percentage or a total key lifetime . . .." Official notice is taken that fixed length renewal periods are old and well known. Therefore it would have been obvious to a person of ordinary skill in the art at

the time the invention was made to set key update periods that are based on a fixed number of days and a percentage of a key's lifetime. This method provides flexibility by giving clients who have keys that have either extremely long or extremely short lifetimes two options as to when to update their keys.

10. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis and Ellison as applied to claim 1 above.

Lewis and Ellison teach the selection of key validity periods on a per client basis. In their system, keys are created by a user and then sent to a certification authority for a certificate. In another implementation of public-key cryptosystems, the certification authority both generates and verifies the public/private key pair, sometimes on request. The previously mentioned RSA key marketing method exemplifies this. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to apply the teachings of Lewis and particularly Ellison to the well-known public key cryptosystem where a certification authority produces the key pair.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached on between 9 AM and 6 PM, Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are (703)

746-7239 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Douglas J. Meislahn
Examiner
Art Unit 2132

DJM
January 23, 2002

GILBERTO BARRON, JR.
PRIMARY EXAMINER
ART UNIT 2132